

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-306118
 (43)Date of publication of application : 05.11.1999

(51)Int.Cl.

G06F 13/00
 G06F 13/00
 G06F 12/00
 G06F 15/00
 H04N 1/21
 H04N 1/44

(21)Application number : 10-110831

(71)Applicant : YAZAKI CORP

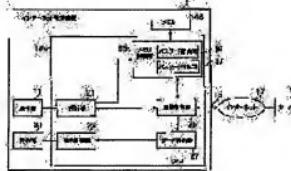
(22)Date of filing : 21.04.1998

(72)Inventor : KATSUTA KEIICHIRO

(54) INTERNET TERMINAL AND IMAGE DISPLAY CONTROL METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To inhibit a minor from browsing detrimental images in an image file that a user downloaded from a home page.
SOLUTION: This device is equipped with a memory 33 stored with image files read out of a server 19 and if an image in an image file is detrimental to a minor, a password addition part 37 adds a password for specifying the user of the image file to the image file and stores it in the memory 33. When the password is inputted from an operation part 11, a password collation part 39 collates the password inputted from the operation part 11 with the password added to the image file in the memory 33 when the image file is read out of the memory 33 and inhibits the image file from being read out when the passwords do not match each other.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-306118

(43)公開日 平成11年(1999)11月5日

(51)Int.Cl. ⁵	識別記号	F I	
G 0 6 F 13/00	3 5 4	G 0 6 F 13/00	3 5 4 D
	3 5 1		3 5 1 G
12/00	5 3 7	12/00	5 3 7 D
15/00	3 3 0	15/00	3 3 0 D
H 0 4 N 1/21		H 0 4 N 1/21	
		審査請求 未請求 請求項の数 6 O L (全 8 頁) 最終頁に続く	

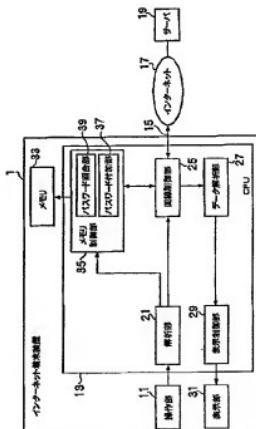
(21)出願番号	特願平10-110831	(71)出願人	000006895 矢崎総業株式会社 東京都港区三田1丁目4番28号
(22)出願日	平成10年(1998)4月21日	(72)発明者	勝田 圭一郎 静岡県裾野市御宿1500 矢崎総業株式会社 内
		(74)代理人	弁理士 三好 秀和 (外8名)

(54)【発明の名称】 インターネット端末装置及び画像表示制御方法

(57)【要約】

【課題】 使用者がホームページからダウンロードした画像ファイルの内、未成年者による有害画像の閲覧を禁止する。

【解決手段】 サーバ19から読み出された画像ファイルを記憶するメモリ33を備え、パスワード付加部37は、画像ファイルの画像が未成年者に対して有害な画像である場合に、画像ファイルの使用者を特定するためのパスワードを画像ファイルに付加してメモリ33に記憶させる。操作部11からパスワードが入力されると、パスワード照合部39は、メモリ33から画像ファイルを読み出す際に、操作部11から入力されたパスワードとメモリ33の画像ファイルに付加されたパスワードとを照合し、パスワードが一致しない場合には画像ファイルの読み出しを禁止する。



【特許請求の範囲】

【請求項1】回線及びインターネットを介してサーバから画像ファイルを読み出して画像を表示部に表示するインターネット端末装置において、

前記サーバから読み出された前記画像ファイルを記憶する記憶手段と、

前記画像ファイルの画像が未成年者に対して有害な画像である場合に、前記画像ファイルの使用者を特定するためのパスワードを前記画像ファイルに付加して前記記憶手段に記憶させるパスワード付加手段と、

前記パスワードを入力する入力手段と、

前記記憶手段から前記画像ファイルを読み出す際に、前記入力手段から入力されたパスワードと前記記憶手段の画像ファイルに付加されたパスワードとを照合するパスワード照合手段と、を備えることを特徴とするインターネット端末装置。

【請求項2】前記パスワード照合手段は、前記入力手段から入力されたパスワードが前記記憶手段の画像ファイルに付加されたパスワードに一致した場合には、前記記憶手段から画像ファイルを読み出し、前記入力手段から入力されたパスワードが前記記憶手段の画像ファイルに付加されたパスワードに一致しない場合には、前記画像ファイルの読み出しを禁止することを特徴とする請求項1記載のインターネット端末装置。

【請求項3】前記パスワード付加手段は、前記画像ファイルに前記パスワードを付加するか否かを確認するための付加確認情報を前記使用者に提示し、この付加確認情報に基づき前記入力手段から前記パスワードが入力された場合に、そのパスワードを前記画像ファイルに付加することを特徴とする請求項1または請求項2記載のインターネット端末装置。

【請求項4】前記パスワード照合手段は、前記記憶手段に記憶された前記画像ファイルに前記パスワードが付加されているか否かを判定し、前記記憶手段に記憶された前記画像ファイルに前記パスワードが付加されている場合には、前記入力手段から入力されたパスワードと前記記憶手段の画像ファイルに付加されたパスワードとを照合することを特徴とする請求項1乃至請求項3のいずれか1項記載のインターネット端末装置。

【請求項5】前記パスワード照合手段は、前記記憶手段に記憶された前記画像ファイルに前記パスワードが付加されているか否かを判定し、前記記憶手段に記憶された前記画像ファイルに前記パスワードが付加されていない場合には、前記記憶手段の画像ファイルを読み出すことを特徴とする請求項1乃至請求項3のいずれか1項記載のインターネット端末装置。

【請求項6】回線及びインターネットを介してサーバから画像ファイルを読み出して画像を表示部に表示させる画像表示制御方法であって、前記サーバから読み出された前記画像ファイルをメモリ

に記憶する記憶ステップと、

前記画像ファイルの画像が未成年者に対して有害な画像である場合に、前記画像ファイルの使用者を特定するためのパスワードを前記画像ファイルに付加して前記メモリに記憶させる付加ステップと、

前記パスワードを入力する入力ステップと、

前記メモリから前記画像ファイルを読み出す際に、前記入力されたパスワードと前記メモリの画像ファイルに付加されたパスワードとを照合する照合ステップと、

前記入力されたパスワードと前記メモリの画像ファイルに付加されたパスワードとが一致する場合に前記メモリの画像ファイルを読み出して前記表示部に表示させる表示制御ステップと、を含むことを特徴とする画像表示制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、公衆回線及びインターネットを介してサーバから画像ファイルを読み出してその画像ファイルの画像を表示するインターネット端末装置に關し、特に使用者がホームページからダウンロードした有害と思われる画像の未成年者の閲覧を禁止するインターネット端末装置及び画像表示制御方法に関するもの。

【0002】

【従来の技術】インターネット通信を行なう従来のインターネット端末装置の一例を図6に示す。このインターネット端末装置の動作を説明すると、まず、操作部11から所望のアドレスを入力すると、そのアドレスは中央処理装置(CPU)113に入力される。そして、そのアドレスは解析部121により解析され、表示制御部129により表示データに変更され、表示器131に表示される。

【0003】また、解析部121で解析されたアドレスに基づき回線制御部125は公衆回線115、及びインターネット117を介して目的のサーバ119に接続する。そして、サーバ119内のデータ(例えば、画像ファイルの画像データ)は、公衆回線115、回線制御部125を介してデータ解析部127で送られる。データ解析部127で解析されたデータは表示制御部129で表示データに変更され、表示器131に表示される。

【0004】このようにインターネット端末装置において、所望のアドレスに対応するサーバ119のホームページにアクセスして画像データをダウンロードして、逐次画像を閲覧することができる。このため、このようなインターネット端末装置を用いて、未成年者等も自由に各種の画像を閲覧することができる。

【0005】

【発明が解決しようとする課題】しかしながら、各種の画像には未成年者にとっては有害な成人向け用の画像もある。このため、従来のインターネット通信システムで

は、図7のフローチャートに示すように、未成年者にとって有害な画像（以下、有害画像と称する。）のホームページへアクセスする（ステップS101）。

【0006】そして、使用者が未成年者かどうかを判定し（ステップS103）、使用者が未成年者でなければ、使用者は、パスワードを入力し（ステップS105）、入力されたパスワードが、予め登録されたパスワードに一致したかどうかを判定することにより、パスワードが正しい（OK）かどうかを判定する（ステップS107）。

【0007】パスワードがOKの場合には、アクセスした画像を表示する（ステップS109）。すなわち、有害画像が表示されるホームページにアクセスした場合には、年齢制限やパスワードによる認証により、未成年者による有害画像の閲覧を禁止させるようになり、また、利用時間の設定によって有害画像の閲覧を禁止せていた。

【0008】しかしながら、使用者がサーバからの有害画像をインターネット端末装置内のメモリにダウンロードしてしまうと、未成年者による有害画像の閲覧を禁止するような情報がメモリに記憶されないため、未成年者は、メモリに記憶された有害画像を容易に読み出して閲覧することができてしまうという問題があった。

【0009】本発明は、使用者がホームページからダウンロードした画像ファイルの内、未成年者による有害画像の閲覧を禁止することができるインターネット端末装置及び画像表示制御方法を提供することを課題とする。

【0010】【課題を解決するための手段】本発明は前記課題を解決するために以下の構成とした。請求項1の発明は、回線及びインターネットを介してサーバから画像ファイルを読み出して画像を表示部に表示するインターネット端末装置において、前記サーバから読み出された前記画像ファイルを記憶する記憶手段と、前記画像ファイルの画像が未成年者に対して有害な画像である場合に、前記画像ファイルの使用者を特定するためのパスワードを前記画像ファイルに付加して前記記憶手段に記憶させるパスワード付加手段と、前記パスワードを入力する入力手段と、前記記憶手段から前記画像ファイルを読み出す際に、前記入力手段から入力されたパスワードと前記記憶手段の画像ファイルに付加されたパスワードとを照合するパスワード照合手段とを備えることを特徴とする。

【0011】請求項1の発明によれば、サーバから読み出された画像ファイルを記憶手段に記憶するときに、画像ファイルの画像が未成年者に対して有害な画像である場合には、パスワード付加手段は、画像ファイルの使用者を特定するためのパスワードを画像ファイルに付加して記憶手段に記憶させる。そして、記憶手段から画像ファイルを読み出す際に、パスワード照合手段は、入力手段から入力されたパスワードと記憶手段の画像ファイル

に付加されたパスワードとを照合する。

【0012】すなわち、使用者が読み出した有害画像を持つ画像ファイルに、パスワードを付加して記憶することによって、未成年者に対して有害な画像の閲覧を禁止することができる。

【0013】請求項2の発明では、前記パスワード照合手段は、前記入力手段から入力されたパスワードが前記記憶手段の画像ファイルに付加されたパスワードに一致した場合には、前記記憶手段から画像ファイルを読み出し、前記入力手段から入力されたパスワードが前記記憶手段の画像ファイルに付加されたパスワードに一致しない場合には、前記画像ファイルの読み出しを禁止することを特徴とする。

【0014】請求項2の発明によれば、入力手段から入力されたパスワードが記憶手段の画像ファイルに付加されたパスワードに一致した場合には、記憶手段から画像ファイルを読み出し、入力手段から入力されたパスワードが記憶手段の画像ファイルに付加されたパスワードに一致しない場合には、画像ファイルの読み出しを禁止するため、未成年者に対して有害な画像の閲覧を禁止することができる。

【0015】請求項3の発明では、前記パスワード付加手段は、前記画像ファイルに前記パスワードを付加するか否かを確認するための付加確認情報を前記使用者に提示し、この付加確認情報に基づき前記入力手段から前記パスワードが入力された場合に、そのパスワードを前記画像ファイルに付加することを特徴とする。

【0016】請求項3の発明によれば、パスワード付加手段が、画像ファイルにパスワードを付加するか否かを確認するための付加確認情報を使用者に提示するため、使用者は、提示された付加確認情報に基づきその画像ファイルの画像が未成年者に対して有害な画像であれば、前記入力手段から前記パスワードを入力し、入力されたパスワードを画像ファイルに付加することができる。

【0017】請求項4の発明では、前記パスワード照合手段は、前記記憶手段に記憶された前記画像ファイルに前記パスワードが付加されているか否かを判定し、前記記憶手段に記憶された前記画像ファイルに前記パスワードが付加されている場合には、前記入力手段から入力されたパスワードと前記記憶手段の画像ファイルに付加されたパスワードとを照合することを特徴とする。

【0018】請求項4の発明によれば、パスワード照合手段は、画像ファイルにパスワードが付加されているか否かを判定し、画像ファイルにパスワードが付加されている場合には、入力手段から入力されたパスワードと記憶手段の画像ファイルに付加されたパスワードとを照合するため、未成年者に対して有害な画像の閲覧を禁止することができる。

【0019】請求項5の発明では、前記パスワード照合手段は、前記記憶手段に記憶された前記画像ファイルに

前記パスワードが付加されているか否かを判定し、前記記憶手段に記憶された前記画像ファイルに前記パスワードが付加されていない場合には、前記記憶手段の画像ファイルを読み出すことを特徴とする。

【0020】請求項5の発明によれば、パスワード照合手段は、画像ファイルにパスワードが付加されているか否かを判定し、画像ファイルにパスワードが付加されていない場合には、記憶手段の画像ファイルを読み出すため、未成年者に関係なくその画像ファイルの画像を閲覧することができる。

【0021】また、請求項6の発明は、回線及びインターネットを介してサーバーから画像ファイルを読み出して画像を表示部に表示させる画像表示制御方法であって、前記サーバーから読み込まれた前記画像ファイルをメモリに記憶する記憶ステップと、前記画像ファイルの画像が未成年者に対して有害な画像である場合に、前記画像ファイルの使用者を特定するためのパスワードを前記画像ファイルに付加して前記メモリに記憶させる付加ステップと、前記パスワードを入力する入力ステップと、前記メモリから前記画像ファイルを読み出す際に、前記入力されたパスワードと前記メモリの画像ファイルに付加されたパスワードとを照合する照合ステップと、前記入力されたパスワードと前記メモリの画像ファイルに付加されたパスワードとが一致する場合に前記メモリの画像ファイルを読み出して前記表示部に表示させる表示制御ステップとを含むことを特徴とする。

【0022】請求項6の発明によれば、サーバーから読み出された画像ファイルをメモリに記憶し、画像ファイルの画像が未成年者に対して有害な画像である場合に、画像ファイルの使用者を特定するためのパスワードを画像ファイルに付加してメモリに記憶させ、メモリから画像ファイルを読み出す際に、入力されたパスワードとメモリの画像ファイルに付加されたパスワードとを照合し、入力されたパスワードとメモリの画像ファイルに付加されたパスワードとが一致する場合にメモリの画像ファイルを読み出して表示部に表示させるため、未成年者の有害な画像の閲覧を禁止することができる。

【0023】

【発明の実施の形態】以下、本発明のインターネット端末装置及び画像表示制御方法の実施の形態を図面を参照して詳細に説明する。

【0024】本発明のインターネット端末装置の実施の形態を説明する。図1に本発明のインターネット端末装置の実施の形態の構成ブロック図を示す。インターネット端末装置1には公衆回線15、インターネット17を介してサーバー19が接続される。

【0025】インターネット端末装置1は、所望の画像ファイルを読み出すためのアドレスや使用者を特定するためのパスワードなどの入力情報を入力する入力手段としての操作部11、この操作部11に接続されるとともに

各部を制御するCPU13、このCPU13に接続され、れる表示器31、CPU13に接続される記憶手段としてのメモリ33を有して構成されている。

【0026】CPU13は、解析部21、回線制御部25、データ解析部27、表示制御部29、メモリ制御部35を有して構成されている。解析部21は、操作部11からの入力情報を解析し、解析された情報を回線制御部25及びメモリ制御部35に出力する。

【0027】回線制御部25は、解析部21で解析された情報がアドレスである場合にそのアドレスに基づき公衆回線15の回線接続を制御し、サーバー19のホームページから所望のアドレスに対応する画像ファイルをダウンロードする。

【0028】データ解析部27は、回線制御部25を介してサーバー19から送られてくる画像ファイルを解析する。表示制御部29は、データ解析部27で解析された画像ファイルを表示データに変更して表示器31に表示させる。

【0029】メモリ制御部35は、使用者がホームページからダウンロードした画像ファイル(未成年者に対して有害な有害画像を有する画像ファイルを含む。)をアドレスに対応させてメモリ33に書き込み制御したり、メモリ33に書き込まれた画像ファイルを読み出し制御したりする。

【0030】メモリ制御部35は、操作部11から入力されたパスワードを、ダウンロードされた画像ファイルに付加してメモリ33に記憶させるパスワード付加手段としてのパスワード付加部37、操作部11から新たに入力されたパスワードとメモリ33に画像ファイルと対応させて記憶されたパスワードとを照合するパスワード照合手段としてのパスワード照合部39を有している。

【0031】パスワード付加部37は、ダウンロードされた画像ファイルにパスワードを付加するか付加しないかを使用者が確認するための付加確認情報を、回線制御部25、データ解析部27、表示制御部29を介して表示器31に表示させることで、付加確認情報を使用者に提示する。

【0032】パスワード付加部37は、使用者が表示器31に表示された付加確認情報を見て、付加確認情報に基づき操作部11からパスワードを入力した場合に、図2に示すように、前記アドレス、操作部から入力されたパスワード、画像ファイルデータをデータファームットとしてメモリ33に記憶させる。

【0033】図3にメモリに記憶された各画像ファイルの記憶内容を示す。図3に示す例では、メモリ33に記憶された複数の画像ファイルの内、画像ファイルデータIMD2にパスワードPW2を付加し、画像ファイルデータIMD3にパスワードPW3を付加し、その他の画像ファイルにはパスワードは付加されていないようになっている。また、複数の画像ファイルデータIMD1～

IMD n は、複数のアドレス AD 1 ~ AD n と 1 対 1 対応で記憶されている。

【0034】パスワード照合部 3 9 は、メモリ 3 3 に記憶された画像ファイルを参照時に、参照すべき画像ファイルにパスワードが付加されているかどうかを判定する。パスワード照合部 3 9 は、参照すべき画像ファイルにパスワードが付加されているとき、操作部 1 1 から入力されたパスワードがメモリ 3 3 に記憶された、参照すべき画像ファイルに付加されたパスワードに一致する場合には、そのパスワードに対応する参照すべき画像ファイルを読み出す。

【0035】パスワード照合部 3 9 は、操作部 1 1 から入力されたパスワードがメモリ 3 3 に記憶された、参照すべき画像ファイルに付加されたパスワードに一致しない場合には、そのパスワードに対応する参照すべき画像ファイルの読み出しを禁止する。

【0036】表示器 3 1 は、メモリ制御部 3 5 によりメモリ 3 3 から読み出された画像ファイルを表示したり、前述した付加確認情報を表示する。

【0037】次に、このように構成された実施の形態のインターネット端末装置の動作、すなわち、画像表示制御方法を図面を参照しながら説明する。この画像表示制御方法は、未成年者に対して有害な有害画像の画面上への表示を禁止するよう制御することを特徴とするものである。この画像表示制御方法は、後述する図 4 のフローチャートの処理及び図 5 のフローチャートの処理により実現される。

【0038】まず、未成年者に対して有害な有害画像のダウンロードを説明する。まず、操作部 1 1 から有害画像のための所要のアドレス (URL ; Uniform Resource Locator) を入力すると、そのアドレスは CPU 1 3 に入力される。そして、そのアドレスは解析部 2 1 により解析され、表示制御部 2 9 により表示データに変更され、表示器 3 1 に表示される。

【0039】また、解析部 2 1 で解析されたアドレスに基づき回線制御部 2 5 は、公衆回線 1 5、及びインターネット 1 7 を介して目的のサーバ 1 9 に接続する。そして、サーバ 1 9 内の有害画像の画像ファイルは、公衆回線 1 5 を介して回線制御部 2 5 に送られる。すなわち、有害画像のダウンロードが行われる。

【0040】次に、図 4 を参照しながら有害画像を有する画像ファイルのメモリへの保存動作を説明する。

【0041】まず、前述したように、回線制御部 2 5 がサーバ 1 9 から有害画像をダウンロードすると (ステップ S 1 1)、メモリ制御部 3 5 は、回線制御部 2 5 から有害画像を有する画像ファイルを取り込む。

【0042】すると、メモリ制御部 3 5 内のパスワード付加部 3 7 は、ダウソードした画像ファイルにパスワードを付加するか付加しないかを使用者が確認するための付加確認情報を、回線制御部 2 5、データ解析部 2

7、表示制御部 2 9 を介して表示器 3 1 に表示させる。~

【0043】表示器 3 1 の画面上には、前記付加確認情報として、例えば、「画像ファイルにパスワードを付加する (YES)、付加しない (NO)」が表示される。すなわち、パスワードを付加するか付加しないかの確認が行われることになる (ステップ S 1 3)。

【0044】そこで、使用者は、画面上のパスワードを付加する (YES) を選択するとともに、操作部 1 1 から使用者を特定するためのパスワードを入力すると (ステップ S 1 5)、そのパスワードは、解析部 2 1 により解釈されて、メモリ制御部 3 5 に入力される。

【0045】そして、パスワード付加部 3 7 は、操作部 1 1 から入力されたパスワードをダウンロードした画像ファイルに付加するため (ステップ S 1 7)、パスワードが付加された画像ファイルは、アドレスに対応させてメモリ 3 3 に保存される (ステップ S 1 9)。これにより、図 2 に示すように、アドレス、パスワード、画像ファイルデータがメモリ 3 3 に記憶される。

【0046】一方、ステップ S 1 3 において、パスワードを付加しない場合、すなわち、操作部 1 1 からパスワードが入力されない場合には、パスワードを付加せず、画像ファイル及びアドレスのみをメモリ 3 3 に保存することになる。

【0047】このようにして、画像ファイルのメモリへの保存動作が終了すると、メモリには図 3 に示すように各画像ファイルが記憶される。図 3 に示す画像ファイルの例では、画像ファイルデータ IMD 2 にパスワード P W 2 を付加し、画像ファイルデータ IMD 3 にパスワード P W 3 を付加しているので、画像ファイルデータ IMD 2 及び画像ファイルデータ IMD 3 が未成年者にとって有害な有害画像であることがわかる。

【0048】次に、メモリ 3 3 に記憶された画像ファイル参照時の動作を図 5 に示すフローチャートを参照して説明する。

【0049】まず、画像ファイル参照時には、参照すべき画像ファイルに対応するアドレスを操作部 1 1 から入力する。そして、入力されたアドレスに対応する参照すべき画像ファイルがメモリ 3 3 に記憶された複数の画像ファイルの中から選択されることになる (ステップ S 3 1)。例えば、アドレス AN 2 を選択すると、図 3 に示すように、アドレス AN 2 に対応する画像ファイルデータ IMD 2 が選択される。

【0050】次に、パスワード照合部 3 9 は、画像ファイルを参照時に、参照すべき画像ファイルにパスワードが付加されているかどうかを判定する (ステップ S 3 3)。参照すべき画像ファイルにパスワードが付加されているとき、使用者は、操作部 1 1 からパスワードを入力する (ステップ S 3 5)。

【0051】さらに、パスワード照合部 3 9 は、操作部 1 1 から入力されたパスワードがメモリ 3 3 に記憶され

た、参照すべき画像ファイルに付加されたパスワードに一致する場合には、そのパスワードに対応する参照すべき画像ファイルを読み出す。すなわち、画像ファイルの参照が行われることになる(ステップS39)。

【0052】そして、メモリ制御部35によりメモリ33から読み出された画像ファイルの画像データは、回線制御部25、データ解析部27、表示制御部29を介して表示器31の画面上に表示される。

【0053】図3に示す例で説明するならば、メモリ33に記憶された、参照すべき画像ファイルデータが“IMD2”であり、パスワードが“PW2”であるとすると、操作部11からパスワードとして“PW2”が入力された場合には、両方のパスワードが一致すると判定されて、参照すべき画像ファイルデータ“IMD2”が読み出されて、画面上に表示されることになる。

【0054】一方、ステップS37において、入力されたパスワードがメモリ33に記憶された、参照すべき画像ファイルに付加されたパスワードに一致しない場合には、パスワード照合部39は、そのパスワードに対応する参照すべき画像ファイルの読み出しを禁止する。すなわち、パスワードが一致しなければ、使用者が未成年者であるとして、参照すべき有害画像の画像ファイルの閲覧を禁止することができる。

【0055】そして、ステップS31の処理に戻り、ステップS31からステップS37の処理を繰り返し行うことになる。

【0056】また、ステップS33において、参照すべき画像ファイルにパスワードが付加されていない場合には、その参照すべき画像ファイルの画像が未成年者に対して有害画像でないため、その画像ファイルは、直ちにメモリ33から読み出されることになる。

【0057】例えば、画像ファイルデータ“IMD1”にはパスワードが付加されていない(図3のパスワードの欄には一で示される。)ので、その画像ファイルデータ“IMD1”は、メモリ33から直ちに読み出される。

【0058】すなわち、パスワードが付加されていない画像ファイルの画像は、未成年者に対して有害な画像でないため、その画像ファイルを容易に参照することができる(ステップS39)。その後の画像ファイルの表示処理は、前述した表示処理と同一処理であるため、ここでは、その説明は省略する。

【0059】このように、実施の形態のインターネット端末装置上にすれば、使用者がホームページからダウンロードしてきた、未成年者にとって有害な画像ファイルに対してパスワードを任意に付加することで、未成年者による有害な画像ファイルの閲覧を禁止することができる。

【0060】なお、本発明は、実施の形態のインターネット端末装置に限定されるものではない。実施の形態で

は、画像ファイルにパスワードを付加するか否かの確認、を行いうための付加確認情報を、表示器31に表示するようになつたが、例えば、前記付加確認情報は、図示しないスピーカなどに出力し、音声により付加確認情報を出力させても良い。そのほか、本発明は、発明の技術的思想を逸脱しない範囲で、種々変形して実施可能であるのは勿論である。

【0061】

【発明の効果】請求項1の発明によれば、サーバから読み出された画像ファイルを記憶手段に記憶するときに、画像ファイルの画像が未成年者に対して有害な画像である場合には、パスワード付加手段は、画像ファイルの使用者を特定するためのパスワードを画像ファイルに付加して記憶手段に記憶させる。記憶手段から画像ファイルを読み出す際に、パスワード照合手段は、入力手段から入力されたパスワードと記憶手段の画像ファイルに付加されたパスワードとを照合する。

【0062】すなわち、使用者が読み出した有害画像を持つ画像ファイルに、パスワードを付加して記憶することによって、未成年者に対して有害な画像の閲覧を禁止することができる。

【0063】請求項2の発明によれば、入力手段から入力されたパスワードが記憶手段の画像ファイルに付加されたパスワードに一致した場合には、記憶手段から画像ファイルを読み出し、入力手段から入力されたパスワードが記憶手段の画像ファイルに付加されたパスワードに一致しない場合には、画像ファイルの読み出しを禁止するため、未成年者に対して有害な画像の閲覧を禁止することができる。

【0064】請求項3の発明によれば、パスワード付加手段が、画像ファイルにパスワードを付加するか否かを確認するための付加確認情報を使用者に提示するため、使用者は、提示された付加確認情報に基づき、その画像ファイルの画像が未成年者に対して有害な画像であれば、前記入力手段から前記パスワードを入力し、入力されたパスワードを画像ファイルに付加することができる。

【0065】請求項4の発明によれば、パスワード照合手段は、画像ファイルにパスワードが付加されているか否かを判定し、画像ファイルにパスワードが付加されている場合には、入力手段から入力されたパスワードと記憶手段の画像ファイルに付加されたパスワードとを照合するため、未成年者に対して有害な画像の閲覧を禁止することができる。

【0066】請求項5の発明によれば、パスワード照合手段は、画像ファイルにパスワードが付加されているか否かを判定し、画像ファイルにパスワードが付加されていない場合には、記憶手段の画像ファイルを読み出すため、未成年者に関係なくその画像ファイルの画像を閲覧することができる。

【0067】請求項6の発明によれば、サーバから読み

出された画像ファイルをメモリに記憶し、画像ファイルの画像が未成年者に対して有害な画像である場合に、画像ファイルの使用者を特定するためのパスワードを画像ファイルに付加してメモリに記憶させ、メモリから画像ファイルを読み出す際に、入力されたパスワードとメモリの画像ファイルに付加されたパスワードとを照合し、入力されたパスワードとが一致する場合にメモリの画像ファイルを読み出して表示部に表示させるため、未成年者の有害な画像の閲覧を禁止することができる。

【図面の簡単な説明】

【図1】本発明のインターネット端末装置の実施の形態の構成ブロック図である。

【図2】画像ファイル保存時にパスワードが付加された画像ファイルを示す図である。

【図3】パスワードが付加された画像ファイル及びパスワードが付加されていない画像ファイルが記憶されたメモリの内容を示す図である。

【図4】実施の形態のインターネット端末装置における画像ファイル保存時の動作を示すフローチャートである。

【図5】実施の形態のインターネット端末装置における画像ファイル参照時の動作を示すフローチャートである。

る。

【図6】従来のインターネット端末装置の一例を示す構成ブロック図である。

【図7】従来のインターネット端末装置における未成年者に対する有害画像の閲覧禁止を説明するためのフローチャートである。

【符号の説明】

1 インターネット端末装置

1 1 操作部

10 1 3 CPU

1 5 公衆回線

1 7 インターネット

1 9 サーバ

2 1 解析部

2 5 回線制御部

2 7 データ解析部

2 9 表示制御部

3 1 表示器

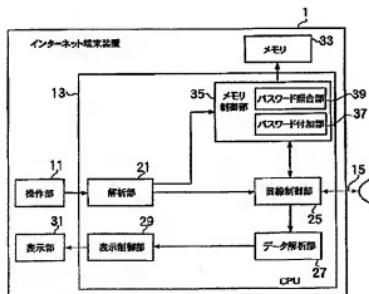
3 3 メモリ

20 3 5 メモリ制御部

3 7 パスワード付加部

3 9 パスワード照合部

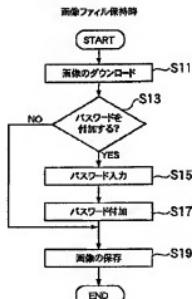
【図1】



【図2】

アドレス	パスワード	画像ファイルデータ
------	-------	-----------

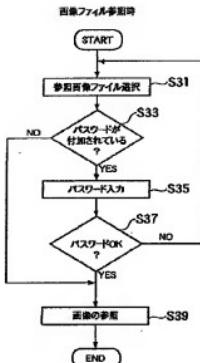
【図4】



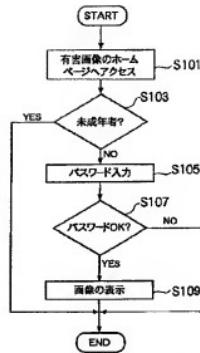
【図3】

アドレス	パスワード	画像ファイルデータ
A01	—	I001
A02	P02	I002
A03	P03	I003
A04	—	I004
⋮	⋮	⋮
Adn	—	In0n

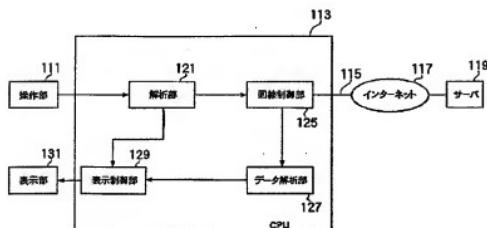
【図5】



【図7】



【図6】



フロントページの続き

(51) Int.C1.°
H04N 1/44

識別記号

F1
H04N 1/44